PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-308249
(43)Date of publication of application : 31.10.2003

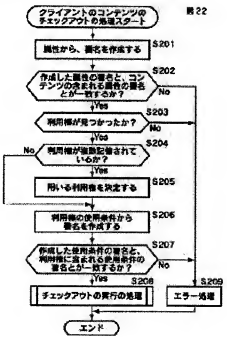
(51)Int.Cl. G06F 12/14
G09C 1/00
H04L 9/14

(21)Application number : 2002-112109
(22)Date of filing : 15.04.2002

(71)Applicant : SONY CORP
(72)Inventor : ISHIGURO RYUJI
TADA KEIKO
FUTAGAMI KISEI

(54) APPARATUS AND METHOD FOR INFORMATION PROCESSING, AND PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To securely prevent contents even in a contents storage device with low capability from illegally being used.
SOLUTION: A CPU selects contents stored in the contents storage device. In a step S202, the CPU verifies a 1st electronic signature added to the contents. A storage part stores a right to use. In a step S203, the CPU retrieves the right to use from the storage part. In a step S207, the CPU verifies a 2nd electronic signature added to the right to use. The CPU generates falsification detection data based upon information included in the right to use. In a step S208, the CPU outputs the use authorization, falsification detection data, and contents to the contents storage device on condition that neither the contents nor the right to use is falsified. This invention is applicable to a client of a DRM system.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－308249
（P2003－308249A）
(43)公開日　平成15年10月31日(2003.10.31)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｚ	５Ｂ０１７
			３１０Ｋ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｄ	
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１	

審査請求　未請求　請求項の数８　ＯＬ　（全 24 頁）

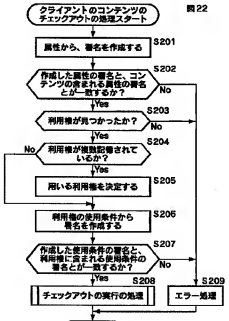
(21)出願番号　特願2002－112109(P2002－112109)
(22)出願日　平成14年４月15日(2002.4.15)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　石黒　隆二
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　多田　恵子
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

最終頁に続く

(54)【発明の名称】　情報処理装置および方法、並びにプログラム

(57)【要約】
【課題】　能力の低いコンテンツ記憶装置においても、コンテンツが不正に利用されるのを確実に防止する。
【解決手段】　CPUは、コンテンツ記憶装置に記憶させるコンテンツを選択する。ステップＳ２０２において、CPUは、コンテンツに付された第１の電子署名の検証を行う。記憶部は、利用権を記憶する。ステップＳ２０３において、CPUは、記憶部から利用権を検索する。ステップＳ２０７において、CPUは、利用権に付された第２の電子署名の検証を行う。CPUは、利用権に含まれている情報に基づき改竄検出データを生成する。ステップＳ２０８において、CPUは、コンテンツおよび利用権が改竄されていないとき、利用権と改竄検出データとコンテンツをコンテンツ記憶装置に出力する。本発明は、DRMシステムのクライアントに適用できる。



1

【特許請求の範囲】

【請求項１】　コンテンツに対応する利用権を基に前記コンテンツの利用を許可する情報処理装置において、

コンテンツ記憶装置に記憶させる前記コンテンツを選択する第１の選択手段と、

前記第１の選択手段により選択された前記コンテンツに付された第１の電子署名の検証を行う第１の検証手段と、

前記第１の選択手段により選択された前記コンテンツの利用を許可する前記利用権を記憶する記憶手段と、

前記記憶手段から前記第１の選択手段により選択された前記コンテンツに対応する前記利用権を検索する検索手段と、

前記検索手段により検索された前記利用権に付された第２の電子署名の検証を行う第２の検証手段と、

前記検索手段により検索された前記利用権に含まれている情報に基づき第１の改竄検出データを生成する第１のデータ生成手段と、

前記第１の検証手段の検証結果、前記第２の検証手段の検証結果により前記コンテンツおよび前記利用権が改竄されていないと判定されたことを条件として、前記利用権と前記第１のデータ生成手段により生成された前記第１の改竄検出データと前記コンテンツを前記コンテンツ記憶装置に出力する第１の出力手段とを備えることを特徴とする情報処理装置。

【請求項２】　前記検索手段により前記利用権が複数検索された場合、検索された複数の前記利用権から１つの前記利用権を選択する第２の選択手段を更に備え、

前記第２の検証手段は前記第２の選択手段により選択された前記利用権に付された前記電子署名の検証を行い、

前記第１のデータ生成手段は前記第２の選択手段により選択された前記利用権に含まれている情報に基づき前記第１の改竄検出データを生成することを特徴とする請求項１に記載の情報処理装置。

【請求項３】　前記第１の選択手段により選択された前記コンテンツを前記コンテンツ記憶装置に対応するフォーマットに変換する変換手段を更に備え、

前記第１の出力手段は前記変換手段により変換された前記コンテンツを前記コンテンツ記憶装置に出力することを特徴とする請求項１に記載の情報処理装置。

【請求項４】　前記コンテンツに対応する前記利用権を前記コンテンツ記憶装置に対応するフォーマットに変換する変換手段を更に備え、

前記第１のデータ生成手段により生成される前記第１の改竄検出データは前記変換手段により変換された前記利用権に基づく改竄検出データであることを特徴とする請求項１に記載の情報処理装置。

【請求項５】　前記第１のデータ生成手段が生成する前記第１の改竄検出データは前記利用権に含まれる使用条件に基づいて生成されることを特徴とする請求項１に記載の情報処理装置。

2

【請求項６】　前記コンテンツ記憶装置から、前記コンテンツ記憶装置に記憶されている前記コンテンツに対応する前記利用権に基づいて前記第１のデータ生成手段により生成された前記第１の改竄検出データ全てを取得する取得手段と、

前記取得手段により取得された前記第１の改竄検出データ全体に基づいて第２の改竄検出データを生成する第２のデータ生成手段と、

前記第２のデータ生成手段により生成された前記第２の改竄検出データを前記コンテンツ記憶装置に出力する第２の出力手段とを更に備えることを特徴とする請求項１に記載の情報処理装置。

【請求項７】　コンテンツに対応する利用権を基に前記コンテンツの利用を許可する情報処理方法において、

コンテンツ記憶装置に記憶させる前記コンテンツを選択する選択ステップと、

前記選択ステップの処理により選択された前記コンテンツに付された第１の電子署名の検証を行う第１の検証ステップと、

前記選択ステップの処理により選択された前記コンテンツの利用を許可する前記利用権の記憶手段への記憶を制御する記憶制御ステップと、

前記記憶手段から前記選択ステップの処理により選択された前記コンテンツに対応する前記利用権を検索する検索ステップと、

前記検索ステップの処理により検索された前記利用権に付された第２の電子署名の検証を行う第２の検証ステップと、

前記検索ステップの処理により検索された前記利用権に含まれている情報に基づき改竄検出データを生成するデータ生成ステップと、

前記第１の検証ステップの処理の検証結果、前記第２の検証ステップの処理の検証結果により前記コンテンツおよび前記利用権が改竄されていないと判定されたことを条件として、前記利用権と前記データ生成ステップの処理により生成された前記改竄検出データと前記コンテンツを前記コンテンツ記憶装置に出力する出力ステップとを含むことを特徴とする情報処理方法。

【請求項８】　コンテンツに対応する利用権を基に前記コンテンツの利用を許可する情報処理を制御するコンピュータに、

コンテンツ記憶装置に記憶させる前記コンテンツを選択する選択ステップと、

前記選択ステップの処理により選択された前記コンテンツに付された第１の電子署名の検証を行う第１の検証ステップと、

前記選択ステップの処理により選択された前記コンテンツの利用を許可する前記利用権の記憶手段への記憶を制御する記憶制御ステップと、

前記記憶手段から前記選択ステップの処理により選択された前記コンテンツに対応する前記利用権を検索する検索ステップと、

前記検索ステップの処理により検索された前記利用権に付された第２の電子署名の検証を行う第２の検証ステップと、

前記検索ステップの処理により検索された前記利用権に含まれている情報に基づき改竄検出データを生成するデータ生成ステップと、

前記第１の検証ステップの処理の検証結果、前記第２の検証ステップの処理の検証結果により前記コンテンツおよび前記利用権が改竄されていないと判定されたことを条件として、前記利用権と前記データ生成ステップの処理により生成された前記改竄検出データと前記コンテンツを前記コンテンツ記憶装置に出力する出力ステップとを実行させることを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報処理装置および方法、並びにプログラムに関し、特に、コンテンツとその利用権が別々に配布される著作権管理システムにおけるコンテンツを、著作権を保護しつつ、他の装置と受け渡しできるようにした、情報処理装置および方法、並びにプログラムに関する。

【０００２】

【従来の技術】最近、インターネットを介して、音楽データや画像データ等のコンテンツをユーザーに配信するシステムが実現されている。

【０００３】

【発明が解決しようとする課題】このような、著作物の著作権を保護するための従来のDRM（Digital Rights Management）システムにおいては、端末機の能力にかかわらず、同一の保護方式を用いているので、特に、能力の低い端末装置またはコンテンツ記憶装置において、コンテンツの不正な利用を防止することは困難であった。

【０００４】また、利用権とコンテンツとを別々に配布するシステムにおいては、端末装置またはコンテンツ記憶装置において、両者の正当性を検証し、マッチングを行う処理は負荷が大きく、困難であった。例えば、コンテンツを処理能力の低い端末装置で、コンテンツに対応する利用権を保持していることを探し出し、その正当性を検証した上で、そのコンテンツの利用を許可するということを実現するのは困難であった。

【０００５】本発明はこのような状況に鑑みてなされたものであり、能力の低いコンテンツ記憶装置においても、コンテンツを利用できるようにすると共に、コンテンツが不正に利用されるのを確実に防止することができるようにするものである。

【０００６】

【課題を解決するための手段】本発明の情報処理装置

は、コンテンツ記憶装置に記憶させるコンテンツを選択する第１の選択手段と、第１の選択手段により選択されたコンテンツに付された第１の電子署名の検証を行う第１の検証手段と、第１の選択手段により選択されたコンテンツの利用を許可する利用権を記憶する記憶手段と、記憶手段から第１の選択手段により選択されたコンテンツに対応する利用権を検索する検索手段と、検索手段により検索された利用権に付された第２の電子署名の検証を行う第２の検証手段と、検索手段により検索された利用権に含まれている情報に基づき第１の改竄検出データを生成する第１のデータ生成手段と、第１の検証手段の検証結果、第２の検証手段の検証結果によりコンテンツおよび利用権が改竄されていないと判定されたことを条件として、利用権と第１のデータ生成手段により生成された第１の改竄検出データとコンテンツをコンテンツ記憶装置に出力する第１の出力手段とを備えることを特徴とする。

【０００７】情報処理装置は、検索手段により利用権が複数検索された場合、検索された複数の利用権から１つの利用権を選択する第２の選択手段を更に設け、第２の検証手段は第２の選択手段により選択された利用権に付された電子署名の検証を行い、第１のデータ生成手段は第２の選択手段により選択された利用権に含まれている情報に基づき第１の改竄検出データを生成するようにすることができる。

【０００８】情報処理装置は、第１の選択手段により選択されたコンテンツをコンテンツ記憶装置に対応するフォーマットに変換する変換手段を更に設け、第１の出力手段は変換手段により変換されたコンテンツをコンテンツ記憶装置に出力するようにすることができる。

【０００９】情報処理装置は、コンテンツに対応する利用権をコンテンツ記憶装置に対応するフォーマットに変換する変換手段を更に設け、第１のデータ生成手段により生成される第１の改竄検出データは変換手段により変換された利用権に基づく改竄検出データとすることができる。

【００１０】第１のデータ生成手段が生成する第１の改竄検出データは利用権に含まれる使用条件に基づいて生成されるようにすることができる。

【００１１】情報処理装置は、コンテンツ記憶装置から、コンテンツ記憶装置に記憶されているコンテンツに対応する利用権に基づいて第１のデータ生成手段により生成された第１の改竄検出データ全てを取得する取得手段と、取得手段により取得された第１の改竄検出データ全体に基づいて第２の改竄検出データを生成する第２のデータ生成手段と、第２のデータ生成手段により生成された第２の改竄検出データをコンテンツ記憶装置に出力する第２の出力手段とを更に設けることができる。

【００１２】本発明の情報処理方法は、コンテンツ記憶装置に記憶させるコンテンツを選択する選択ステップ

と、選択ステップの処理により選択されたコンテンツに付された第１の電子署名の検証を行う第１の検証ステップと、選択ステップの処理により選択されたコンテンツの利用を許可する利用権の記憶手段への記憶を制御する記憶制御ステップと、記憶手段から選択ステップの処理により選択されたコンテンツに対応する利用権を検索する検索ステップと、検索ステップの処理により検索された利用権に付された第２の電子署名の検証を行う第２の検証ステップと、検索ステップの処理により検索された利用権に含まれている情報に基づき改竄検出データを生成するデータ生成ステップと、第１の検証ステップの処理の検証結果、第２の検証ステップの処理の検証結果によりコンテンツおよび利用権が改竄されていないと判定されたことを条件として、利用権とデータ生成ステップの処理により生成された改竄検出データとコンテンツをコンテンツ記憶装置に出力する出力ステップとを含むことを特徴とする。

【００１３】本発明のプログラムは、コンピュータに、コンテンツ記憶装置に記憶させるコンテンツを選択する選択ステップと、選択ステップの処理により選択されたコンテンツに付された第１の電子署名の検証を行う第１の検証ステップと、選択ステップの処理により選択されたコンテンツの利用を許可する利用権の記憶手段への記憶を制御する記憶制御ステップと、記憶手段から選択ステップの処理により選択されたコンテンツに対応する利用権を検索する検索ステップと、検索ステップの処理により検索された利用権に付された第２の電子署名の検証を行う第２の検証ステップと、検索ステップの処理により検索された利用権に含まれている情報に基づき改竄検出データを生成するデータ生成ステップと、第１の検証ステップの処理の検証結果、第２の検証ステップの処理の検証結果によりコンテンツおよび利用権が改竄されていないと判定されたことを条件として、利用権とデータ生成ステップの処理により生成された改竄検出データとコンテンツをコンテンツ記憶装置に出力する出力ステップとを実行させることを特徴とする。

【００１４】本発明の情報処理装置および方法、並びにプログラムにおいては、コンテンツ記憶装置に記憶させるコンテンツが選択され、選択されたコンテンツに付された第１の電子署名の検証が行われ、選択されたコンテンツの利用を許可する利用権が記憶される。そして、記憶手段から選択されたコンテンツに対応する利用権が検索され、検索された利用権に付された第２の電子署名の検証が行われる。検索された利用権に含まれている情報に基づき改竄検出データが生成される。さらに、第１の検証結果、第２の検証結果によりコンテンツおよび利用権が改竄されていないと判定されたことを条件として、利用権と改竄検出データとコンテンツがコンテンツ記憶装置に出力される。

【００１５】コンテンツは、音声、画像、またはテキストなどの情報の方式にかかわらず有用な情報であれば良い。

【００１６】電子署名は、生成の方式を問わず、正当性を保証するための情報であれば良い。

【００１７】

【発明の実施の形態】図１は、本発明を適用したコンテンツ提供システムの構成を示している。インターネット２には、クライアント１－１，１－２（以下、これらのクライアントを個々に区別する必要がない場合、単にクライアント１と称する）が接続されている。この例においては、クライアントが２台のみ示されているが、インターネット２には、任意の台数のクライアントが接続される。

【００１８】また、インターネット２には、クライアント１に対してコンテンツを提供するコンテンツサーバ３、コンテンツサーバ３が提供するコンテンツを利用するのに必要な利用権をクライアント１に対して付与するライセンスサーバ４、およびクライアント１が利用権を受け取った場合に、そのクライアント１に対して課金処理を行う課金サーバ５が接続されている。

【００１９】これらのコンテンツサーバ３，ライセンスサーバ４，および課金サーバ５も、任意の台数、インターネット２に接続される。

【００２０】図２はクライアント１の構成を表している。

【００２１】図２において、CPU（Central Processing Unit）２１は、ROM（Read Only Memory）２２に記憶されているプログラム、または記憶部２８からRAM（Random Access Memory）２３にロードされたプログラムに従って各種の処理を実行する。タイマ２０は、計時動作を行い、時刻情報をCPU２１に供給する。RAM２３にはまた、CPU２１が各種の処理を実行する上において必要なデータなども適宜記憶される。

【００２２】暗号化復号部２４は、コンテンツデータを暗号化するとともに、既に暗号化されているコンテンツデータを復号する処理を行う。コーデック部２５は、例えば、ATRAC（Adaptive Transform Acoustic Coding）３方式などでコンテンツデータをエンコードし、入出力インタフェース３２を介してドライブ３０に接続されている半導体メモリ４４に供給し、記録させる。あるいはまた、コーデック部２５は、ドライブ３０を介して半導体メモリ４４より読み出した、エンコードされているデータをデコードする。

【００２３】半導体メモリ４４は、例えば、メモリースティック（商標）などにより構成される。

【００２４】CPU２１、ROM２２、RAM２３、暗号化復号部２４、およびコーデック部２５は、バス３１を介して相互に接続されている。このバス３１にはまた、入出力インタフェース３２も接続されている。

【００２５】入出力インタフェース３２には、キーボー

ド、マウスなどよりなる入力部２６、CRT、LCDなどよりなるディスプレイ、並びにスピーカなどよりなる出力部２７、ハードディスクなどより構成される記憶部２８、モデム、ターミナルアダプタなどより構成される通信部２９が接続されている。通信部２９は、インターネット２を介しての通信処理を行う。通信部２９はまた、他のクライアントとの間で、アナログ信号またはデジタル信号の通信処理を行う。

【００２６】入出力インタフェース３２にはまた、必要に応じてドライブ３０が接続され、磁気ディスク４１、光ディスク４２、光磁気ディスク４３、或いは半導体メモリ４４などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部２８にインストールされる。

【００２７】なお、図示は省略するが、コンテンツサーバ３、ライセンスサーバ４、課金サーバ５も、図２に示したクライアント１と基本的に同様の構成を有するコンピュータにより構成される。そこで、以下の説明においては、図２の構成は、コンテンツサーバ３、ライセンスサーバ４、課金サーバ５などの構成としても引用される。

【００２８】なお、図示は省略するが、PD（Portable Device）も、図２に示したクライアント１と基本的に同様の構成を有するコンピュータにより構成される。

【００２９】次に、図３のフローチャートを参照して、クライアント１がコンテンツサーバ３からコンテンツの提供を受ける処理について説明する。

【００３０】ユーザが、入力部２６を操作することでコンテンツサーバ３に対するアクセスを指令すると、CPU２１は、ステップＳ１において、通信部２９を制御し、インターネット２を介してコンテンツサーバ３にアクセスさせる。ステップＳ２において、ユーザが、入力部２６を操作して、提供を受けるコンテンツを指定すると、CPU２１は、この指定情報を受け取り、通信部２９から、インターネット２を介してコンテンツサーバ３に、指定されたコンテンツのコンテンツIDを通知する。図４のフローチャートを参照して後述するように、この通知を受けたコンテンツサーバ３は、暗号化されたコンテンツデータを含むコンテンツを送信してくるので、ステップＳ３において、CPU２１は、通信部２９を介して、このコンテンツデータを受信すると、ステップＳ４において、その暗号化されているコンテンツデータを記憶部２８を構成するハードディスクに供給し、記憶させる。

【００３１】次に、図４のフローチャートを参照して、クライアント１の以上の処理に対応するコンテンツサーバ３のコンテンツ提供処理について説明する。なお、以下の説明において、図２のクライアント１の構成は、コンテンツサーバ３の構成としても引用される。

【００３２】ステップＳ２１において、コンテンツサーバ３のCPU２１は、インターネット２から通信部２９を介してクライアント１よりアクセスを受けるまで待機し、アクセスを受けたと判定したとき、ステップＳ２２に進み、クライアント１からIDが送信されてきたコンテンツIDを取り込む。このコンテンツIDは、クライアント１が、図３のステップＳ２において通知してきた情報である。

【００３３】ステップＳ２３において、コンテンツサーバ３のCPU２１は、記憶部２８に記憶されているコンテンツの中から、ステップＳ２２の処理で取り込まれたコンテンツIDで指定されたコンテンツデータを読み出す。CPU２１は、ステップＳ２４において、記憶部２８から読み出されたコンテンツデータを、暗号化復号部２４に供給し、コンテンツキーKcを用いて暗号化させる。

【００３４】記憶部２８に記憶されているコンテンツデータは、コーデック部２５により、既にATRAC３方式によりエンコードされているので、このエンコードされているコンテンツデータが暗号化されることになる。

【００３５】なお、もちろん、記憶部２８に予め暗号化した状態でコンテンツデータを記憶させることができる。この場合には、ステップＳ２４の処理は省略することが可能である。

【００３６】次に、ステップＳ２５において、コンテンツサーバ３のCPU２１は、暗号化したコンテンツデータを伝送するフォーマットを構成するヘッダに、暗号化されているコンテンツを復号するのに必要なキー情報（図５を参照して後述するEKBとK_{enc}（Kc））を付加する。そして、ステップＳ２６において、コンテンツサーバ３のCPU２１は、ステップＳ２４の処理で暗号化したコンテンツと、ステップＳ２５の処理でキー情報を付加したヘッダとをフォーマット化したデータを、通信部２９から、インターネット２を介して、アクセスしてきたクライアント１に送信する。

【００３７】図５は、このようにして、コンテンツサーバ３からクライアント１にコンテンツが供給される場合のフォーマットの構成を表している。同図に示されるように、このフォーマットは、ヘッダ（Header）とデータ（Data）とにより構成される。

【００３８】ヘッダには、コンテンツ情報（Content information）、URL(Uniform Resource Locator)、イネーブリングキーブロック（有効化キーブロック）（EKB（Enabling Key Block））、EKBから生成されたK_{enc}を用いて暗号化されたコンテンツキーKcとしてのデータK_{enc}（Kc）、コンテンツの属性（Attributes）、および署名（Signatures）が配置されている。なお、EKBについては、図１３および図１４を参照して後述する。

【００３９】コンテンツ情報には、データとしてフォーマット化されているコンテンツデータを識別するための識別情報としてのコンテンツID（CID）、そのコンテンツのコーデックの方式などの情報が含まれている。

【００４０】URLは、そのコンテンツを利用するために

必要な利用権を取得するときアクセスするアドレス情報であり、図１のシステムの場合、具体的には、利用権を受けるために必要なライセンスサーバ４のアドレスである。

【００４１】コンテンツの属性は、コンテンツの関する情報であり、コンテンツの属性には、コンテンツID、コンテンツの提供者を識別するための識別情報としてのレコードカンパニーID、アーティストを識別するための識別情報としてのアーティストIDなどが含まれる。本実施の形態では、属性は利用権の対象となるコンテンツを特定するために用いられる。

【００４２】署名は、コンテンツの属性に対応する電子署名である。

【００４３】データは、任意の数の暗号化ブロック（Encryption Block）により構成される。各暗号化ブロックは、イニシャルベクトル（IV（Initial Vector））、シード（Seed）、およびコンテンツデータをキーK'cで暗号化したデータE$_{K'c}$（data）により構成されている。

【００４４】キーK'cは、次式により示されるように、コンテンツキーKcと、乱数で設定される値Seedをハッシュ関数に適用して演算された値により構成される。K'c＝Hash(Kc, Seed)

【００４５】イニシャルベクトルIVとシードSeedは、各暗号化ブロック毎に異なる値に設定される。

【００４６】この暗号化は、コンテンツのデータを８バイト単位で区分して、８バイト毎に行われる。後段の８バイトの暗号化は、前段の８バイトの暗号化の結果を利用して行われるCBC（Cipher Block Chaining）モードで行われる。

【００４７】CBCモードの場合、最初の８バイトのコンテンツデータを暗号化するとき、その前段の８バイトの暗号化結果が存在しないため、最初の８バイトのコンテンツデータを暗号化するときは、イニシャルベクトルIVを初期値として暗号化が行われる。

【００４８】このCBCモードによる暗号化を行うことで、１つの暗号化ブロックが解読されたとしても、その影響が、他の暗号化ブロックにおよぶことが抑制される。

【００４９】また、暗号方式についてはこれに限らない。

【００５０】以上のようにして、クライアント１は、コンテンツサーバ３からコンテンツを無料で、自由に取得することができる。従って、コンテンツそのものは、大量に、配布することが可能となる。

【００５１】しかしながら、各クライアント１は、取得したコンテンツを利用するとき、そのコンテンツの利用が許可されていることを示す利用権を保持している必要がある。そこで、図６を参照して、クライアント１がコンテンツを再生する場合の処理について説明する。

【００５２】ステップＳ４１において、クライアント１

のCPU２１は、ユーザが入力部２６を操作することで指示したコンテンツの識別情報（CID）を取得する。この識別情報は、例えば、コンテンツのタイトルや、記憶されている各コンテンツ毎に付与されている番号などにより構成される。

【００５３】そして、CPU２１は、コンテンツが指示されると、そのコンテンツの属性（Attributes）を読み取る。この属性（Attributes）は、図５に示されるように、コンテンツのヘッダに記述されているものである。

【００５４】次に、ステップＳ４２に進み、CPU２１は、ステップＳ４１で読み取られた属性（Attributes）が各利用権に含まれているコンテンツ条件を満たすような利用権が、クライアント１に既に取得され、記憶部２８に記憶されているか否かを判定する。まだ、利用権が取得されていない場合には、ステップＳ４３に進み、CPU２１は、利用権取得処理を実行する。この利用権取得処理の詳細は、図７のフローチャートを参照して後述する。

【００５５】ステップＳ４２において、利用権が既に取得されていると判定された場合、または、ステップＳ４３において、利用権取得処理が実行された結果、利用権が取得された場合、ステップＳ４４に進み、CPU２１は、取得されている利用権は有効期限内のものであるか否かを判定する。利用権が有効期限内のものであるか否かは、利用権の内容として規定されている期限（後述する図８参照）と、タイマ２０により計時されている現在日時と比較することで判断される。利用権の有効期限が既に満了していると判定された場合、CPU２１は、ステップＳ４５に進み、利用権更新処理を実行する。

【００５６】ステップＳ４４において、利用権はまだ有効期限内であると判定された場合、または、ステップＳ４５において、利用権が更新された場合、ステップＳ４６に進み、CPU２１は記憶部２８に記憶されている、利用権に含まれる使用条件及び使用状態（後述する）を読み出し、再生の条件を満たしているかどうかを判定する。

【００５７】ステップＳ４６において、利用権に含まれる使用条件、及び使用状態に基づき、再生が許可されると判断された場合には、ステップＳ４７に進み、CPU２１は、暗号化されているコンテンツデータを記憶部２８から読み出し、RAM２３に格納させる。そして、ステップＳ４８において、CPU２１は、RAM２３に記憶された暗号化コンテンツデータを、図５のデータに配置されている暗号化ブロック単位で、暗号化復号部２４に供給し、コンテンツキーKcを用いて復号させる。

【００５８】コンテンツキーKcを得る方法の具体例は、図１３および図１４を参照して後述するが、デバイスノードキー（DNK）を用いて、EKB（図５）に含まれるキーK$_{EKBc}$を得ることができ、そのキーK$_{EKBc}$を用いて、データK$_{EKBc}$（Kc）（図５）から、コンテンツキーKcを得

ることができる。

【００５９】CPU２１は、さらに、ステップＳ４９において、暗号化復号部２４により復号されたコンテンツデータをコーデック部２５に供給し、デコードさせる。そして、コーデック部２５によりデコードされたデータを、CPU２１は、入出力インタフェース３２から出力部２７に供給し、D/A変換させ、スピーカから出力させる。

【００６０】ステップＳ４６において、利用権に含まれる使用条件、及び使用状態に基づき、再生が許可されないと判断された場合、コンテンツを出力しないで、処理は終了する。

【００６１】次に、図７のフローチャートを参照して、図８のステップＳ４３で行われる利用権取得処理の詳細について説明する。

【００６２】クライアント１は、事前にライセンスサーバ５に登録することにより、リーフID、DNK(Device Node Key)、クライアント１の秘密鍵・公開鍵のペア、ライセンスサーバの公開鍵、及び各公開鍵の証明書を含むサービスデータを取得しておく。

【００６３】リーフIDは、クライアント毎に割り当てられた識別情報を表し、DNKは、コンテンツに含まれるEKB（有効化キーブロック）によって暗号化されているコンテンツキーKcを復号するのに必要なデバイスノードキーである（図１０を参照して後述する）。

【００６４】最初にステップＳ６１において、CPU２１は、コンテンツのヘッダに記述されているURLを取得する。上述したように、このURLは、そのコンテンツを利用するために必要な利用権を取得するときアクセスすべきアドレスである。そこで、ステップＳ６２において、CPU２１は、ステップＳ６１で取得したURLにアクセスする。具体的には、通信部２９によりインターネット２を介してライセンスサーバ４にアクセスが行われる。このとき、ライセンスサーバ４は、クライアント１に対して、利用権のリストを送信するとともに、購入する利用権（コンテンツを使用するのに必要な利用権）を指定する利用権指定情報、並びにユーザIDとパスワードの入力を要求してくる（後述する図９のステップＳ１０２）。CPU２１は、この要求を出力部２７の表示部に表示させる。ユーザは、この表示に基づいて、入力部２６を操作して、利用権指定情報、ユーザID、およびパスワードを入力する。なお、このユーザIDとパスワードは、クライアント１のユーザが、インターネット２を介してライセンスサーバ４にアクセスし、事前に取得しておいたものである。

【００６５】CPU２１は、ステップＳ６３，Ｓ６４において、入力部２８から入力された利用権指定情報を取り込むとともに、ユーザIDとパスワードを取り込む。CPU２１は、ステップＳ６５において、通信部２９を制御し、入力されたユーザIDとパスワードを、利用権指定情報及びサービスデータ（後述する）に含まれるリーフIDを含む利用権要求をインターネット２を介してライセンスサーバ４に送信させる。

【００６６】ライセンスサーバ４は、図９を参照して後述するように、ユーザIDとパスワード、並びに利用権指定情報に基づいて利用権を送信してくる（ステップＳ１０９）か、または、条件が満たされない場合には、利用権を送信してこない（ステップＳ１１２）。

【００６７】ステップＳ６６において、CPU２１は、ライセンスサーバ４から利用権が送信されてきたか否かを判定し、利用権が送信されてきた場合には、ステップＳ６７に進み、その利用権を記憶部２８に供給し、記憶させる。

【００６８】ステップＳ６６において、利用権が送信されて来ないと判定した場合、CPU２１は、ステップＳ６８に進み、エラー処理を実行する。具体的には、CPU２１は、コンテンツを利用するための利用権が得られないので、コンテンツの再生処理を禁止する。

【００６９】以上のようにして、各クライアント１は、コンテンツを利用するために必要な利用権を取得して、初めて、そのコンテンツを使用することが可能となる。

【００７０】なお、図７の利用権取得処理は、各ユーザがコンテンツを取得する前に、予め行っておくようにすることも可能である。

【００７１】クライアント１に提供される利用権は、例えば、図８に示されるように、使用条件、リーフIDおよび電子署名などを含んでいる。

【００７２】バージョンは、メジャーバージョンおよびマイナーバージョンをドットで区切って、利用権のバージョンを記述する情報である。

【００７３】プロファィルは、１０進の整数値から記述され、利用権の記述方法に対する制限を規定する情報である。

【００７４】利用権IDは、１６進定数で記述される、利用権を識別するための識別情報である。

【００７５】作成日時は、利用権が作成された日時を示す。

【００７６】有効期限は、利用権の有効期限を示す。９９９９年２３時５９分５９秒である有効期限は、有効期限に制限がないことを示す。

【００７７】使用条件には、その利用権に基づいて、コンテンツを使用することが可能な使用期限、その利用権に基づいて、コンテンツを再生することが可能な再生期限、コンテンツの最大再生回数、その利用権に基づいて、コンテンツをコピーすることが可能な回数（許されるコピー回数）、最大チェックアウト回数、その利用権に基づいて、コンテンツをCD-RIC記録することができるか否か、PD（Portable Device）にコピーすることが可能な回数、利用権の移動の可否、使用ログをとる義務の有無等を示す情報が含まれる。

【００７８】使用条件の電子署名は、使用条件に対応する、電子署名である。

【００７９】定数は、使用条件または使用状態で参照される定数である。

【００８０】リーフＩＤは、クライアントを識別するための識別情報である。

【００８１】電子署名は、利用権全体に対応する、電子署名である。

【００８２】証明書は、ライセンスサーバの公開鍵を含む証明書である。

【００８３】また、クライアント１の記憶部２８には、利用権の使用条件とあわせて、コンテンツや利用権の状態を表す情報である使用状態が記憶される。使用状態には、対応する利用権に基づいてコンテンツを再生した回数、コンテンツをコピーした回数、コンテンツをチェックアウトした回数、コンテンツを初めて再生した日時、コンテンツをＣＤ-ＲＷに記録した回数、その他コンテンツあるいは利用権に関する履歴情報等を示す情報が含まれる。

【００８４】図６のステップＳ４６の再生の条件の判定は、利用権に含まれる使用条件と、記憶部２８に利用権と共に記憶されている使用状態とを基に行われる。例えば、使用状態に記憶されているコンテンツを再生した回数が、使用条件に含まれるコンテンツ最大再生回数より少ない場合には、再生の条件が満たされていると判定される。

【００８５】次に、図９のフローチャートを参照して、図７のクライアント１の利用権取得処理に対応して実行されるライセンスサーバ４の利用権提供処理について説明する。なお、この場合においても、図２のクライアント１の構成は、ライセンスサーバ４の構成として引用される。

【００８６】ステップＳ１０１において、ライセンスサーバ４のＣＰＵ２１は、クライアント１よりアクセスを受けるまで待機し、アクセスを受けたとき、ステップＳ１０２に進み、アクセスしてきたクライアント１に対して、各利用権に関する情報を含む利用権のリストを送信するとともに、ユーザＩＤとパスワード、並びに、利用権指定情報の送信を要求する。上述したようにして、クライアント１から、図７のステップＳ６５の処理で、ユーザＩＤとパスワード、リーフＩＤ並びに利用権指定情報（利用権ＩＤであってもよい）が送信されてきたとき、ライセンスサーバ４のＣＰＵ２１は、通信部２９を介してこれを受信し、取り込む処理を実行する。

【００８７】そして、ライセンスサーバ４のＣＰＵ２１は、ステップＳ１０３において、通信部２９から課金サーバ５にアクセスし、ユーザＩＤとパスワードに対応するユーザの与信処理を要求する。課金サーバ５は、インターネット２を介してライセンスサーバ４から与信処理の要求を受けると、そのユーザＩＤとパスワードに対応するユーザの過去の支払い履歴などを調査し、そのユーザが、過去に利用権の対価の不払いの実績があるか否かなどを調べ、そのような実績がない場合には、利用権の付与を許容する与信結果を送信し、不払いの実績などがある場合には、利用権付与の不許可の与信結果を送信する。

【００８８】ステップＳ１０４において、ライセンスサーバ４のＣＰＵ２１は、課金サーバ５からの与信結果が、利用権を付与することを許容する与信結果であるか否かを判定し、利用権の付与が許容されている場合には、ステップＳ１０５に進み、ステップＳ１０２の処理で取り込まれた利用権指定情報に対応する利用権を、記憶部２８に記憶されている利用権の中から取り出す。記憶部２８に記憶されている利用権は、あらかじめ利用権ＩＤ、バージョン、作成日時、有効期限等の情報が記述されている。ステップＳ１０６において、ＣＰＵ２１は、その利用権に受信したリーフＩＤを付加する。さらに、ステップＳ１０７において、ＣＰＵ２１は、ステップＳ１０５で選択された利用権に対応づけられている使用条件を選択する。あるいはまた、ステップＳ１０２の処理で、ユーザから使用条件が指定された場合には、その使用条件が必要に応じて、予め用意されている使用条件に付加される。ＣＰＵ２１は、選択された使用条件を利用権に付加する。使用条件は利用権にあらかじめ付加されていてもよい。

【００８９】ステップＳ１０８において、ＣＰＵ２１はライセンスサーバの秘密鍵により利用権に署名し、ライセンスサーバの公開鍵を含む証明書を利用権に添付し、これにより、図８に示されるような構成の利用権が生成される。

【００９０】次に、ステップＳ１０９に進み、ライセンスサーバ４のＣＰＵ２１は、その利用権（図８に示される構成を有する）を、通信部２９からインターネット２を介してクライアント１に送信させる。

【００９１】ステップＳ１１０においてライセンスサーバ４のＣＰＵ２１は、ステップＳ１０９の処理で、いま送信した利用権（使用条件、リーフＩＤを含む）を、ステップＳ１０２の処理で取り込まれたユーザＩＤとパスワードに対応して、記憶部２８に記憶させる。さらに、ステップＳ１１１において、ＣＰＵ２１は、課金処理を実行する。具体的には、ＣＰＵ２１は、通信部２９から課金サーバ５に、そのユーザＩＤとパスワードに対応するユーザに対する課金処理を要求する。課金サーバ５は、この課金の要求に基づいて、そのユーザに対する課金処理を実行する。上述したように、この課金処理に対して、そのユーザが支払いを行わなかったような場合には、以後、そのユーザは、利用権の付与を要求したとしても、利用権を受けることができないことになる。

【００９２】すなわち、この場合には、課金サーバ５から利用権の付与を不許可とする与信結果が送信されてく

るので、ステップＳ１０４からステップＳ１１２に進み、CPU２１は、エラー処理を実行する。具体的には、ライセンスサーバ４のCPU２１は、通信部２９を制御してアクセスしてきたクライアント１に対して、利用権を付与することができない旨のメッセージを送信し、処理を終了させる。

【００９３】この場合、上述したように、そのクライアント１は利用権を受けることができないので、そのコンテンツを利用するとき（暗号化されたコンテンツデータを復号し、再生するとき）ができないことになる。

【００９４】本発明においては、図１０に示されるように、ブロードキャストインクリプション（Broadcast Encryption）方式の原理に基づいて、デバイスとキーが管理される。キーは、階層ツリー構造とされ、最下段のリーフ（leaf）が個々のデバイス固有のキーに対応する。本発明のシステムに用いられる階層ツリー構造鍵管理については特許公開２００１－３５２３２１号公報に記載されている。図１０の例の場合、番号０から番号１５までの１６個のデバイスに対応するキーが生成される。

【００９５】各キーは、図中丸印で示されるツリー構造の各ノードに対応して規定される。この例では、最上段のルートノードに対応してルートキーKRが、２段目のノードに対応してキーＫ０，Ｋ１が、３段目のノードに対応してキーＫ００乃至Ｋ１１が、第４段目のノードに対応してキーＫ０００乃至キーＫ１１１が、それぞれ対応されている。そして、最下段のノードとしてのリーフ（デバイスノード）に、キーＫ００００乃至Ｋ１１１１が、それぞれ対応されている。

【００９６】階層構造とされているため、例えば、キーＫ００１０とキーＫ００１１の上位のキーは、Ｋ００１とされ、キーＫ０００とキーＫ００１の上位のキーは、Ｋ００とされている。以下同様に、キーＫ００とキーＫ０１の上位のキーは、Ｋ０とされ、キーＫ０とキーＫ１の上位のキーは、KRとされている。

【００９７】コンテンツを利用するキーは、最下段のデバイスノード（リーフ）から、最上段のルートノードまでの１つのパスの各ノードに対応するキーで管理される。例えば、番号３のリーフに対応するデバイスにおいて、コンテンツを利用するためのキーは、キーＫ００１１，Ｋ００１，Ｋ００，Ｋ０，KRを含むパスの各キーで管理される。

【００９８】本発明のシステムにおいては、図１１に示されるように、図１０の原理に基づいて構成されるキーシステムで、デバイスのキーとコンテンツのキーの管理が行われる。図１１の例では、８＋２４＋３２段のノードがツリー構造とされ、ルートノードから下位の８段までの各ノードにカテゴリが対応される。ここにおけるカテゴリとは、例えばメモリースティックなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。そして、このカテゴリノードのうちの１つのノードに、ライセンスを管理するシステムとして本システム（Tシステムと称する）が対応する。

【００９９】すなわち、このTシステムのノードよりさらに下の階層の２４段のノードに対応するキーにより、サービスプロバイダ、あるいはサービスプロバイダが提供するサービスが対応される。この例の場合、これにより、2^{24}（約１６メガ）のサービスプロバイダあるいはサービスを規定することができる。さらに、最も下側の３２段の階層により、2^{32}（約４ギガ）のユーザ（あるいはクライアント１）を規定することができる。最下段の３２段のノードからTシステムのノードまでのパス上の各ノードに対応するキーが、DNK（Device Node Key）を構成し、最下段のリーフに対応するIDがリーフIDとされる。

【０１００】コンテンツを暗号化したコンテンツキーは更新されたルートキーKR'によって暗号化され、上位の階層の更新ノードキーは、その直近の下位の階層の更新ノードキーを用いて暗号化され、ＥＫＢ（図１３および図１４を参照して後述する）内に配置される。ＥＫＢにおける末端から１つ上の段の更新ノードキーはＥＫＢの末端のノードキーあるいはリーフキーによって暗号化され、ＥＫＢ内に配置される。クライアント１は、サービスデータに記述されているＤＮＫのいずれかのキーを用いて、コンテンツデータとともに配布されるＥＫＢ（図１３および図１４）内に記述されている直近の上位の階層の更新ノードキーを復号し、復号して得たキーを用いて、ＥＫＢ内に記述されているさらにその上の階層の更新ノードキーを復号する。以上の処理を順次行うことで、クライアント１は、更新ルートキーKR'を得ることができる。

【０１０１】図１２に階層ツリー構造のカテゴリの分類の具体的な例を示す。図１２において、階層ツリー構造の最上段にはルートキーKR２３０１が設定され、以下の中間段にはノードキー２３０２が設定され、最下段には、リーフキー２３０３が設定される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーからなるデバイスノードキー（ＤＮＫ）を保有する。

【０１０２】最上段から第Ｍ段目（図１１の例では、Ｍ＝８）の所定のノードがカテゴリノードＦ２３０４として設定される。すなわち第Ｍ段目のノードの各々が特定カテゴリのデバイス設定ノードとされる。第Ｍ段の１つのノードを頂点としてＭ＋１段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとされる。

【０１０３】例えば図１２の第Ｍ段目の１つのノード２３０５にはカテゴリ［メモリースティック（商標）］が設定され、このノード以下に連なるノード、リーフはメモリスティックを使用した様々なデバイスを含むカテゴ

リ専用のノードまたはリーフとして設定される。すなわち、ノード２３０５以下が、メモリースティックのカテゴリに定義されるデバイスの関連ノード、およびリーフの集合として定義される。

【０１０４】さらに、Ｍ段から数段分下位の段をサブカテゴリノード２３０６として設定することができる。図１２の例では、カテゴリ［メモリースティック］ノード２３０５の２段下のノードに、メモリースティックを使用したデバイスのカテゴリに含まれるサブカテゴリノードとして、［再生専用器］のノード２３０６が設定されている。さらに、サブカテゴリノードである再生専用器のノード２３０８以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード２３０７が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる［ＰＨＳ］ノード２３０８と、［携帯電話］ノード２３０９が設定されている。

【０１０５】さらに、カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えばあるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位（これらを総称して以下、エンティティと呼ぶ）で設定することが可能である。例えば１つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器ＸＹＺ専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器ＸＹＺに、その頂点ノード以下の下段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化キーブロック（ＥＫＢ）を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

【０１０６】このように、１つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の１つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キーブロック（ＥＫＢ）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノード以下に属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずにキー更新を実行することができる。

【０１０７】また、ある時点ｔにおいて、デバイス３の所有する鍵Ｋ００１１,Ｋ００１,Ｋ００,Ｋ０,ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキーＫ００１,Ｋ００,Ｋ０,ＫＲを、それぞれ新たな鍵Ｋ（ｔ）００１,Ｋ（ｔ）００,Ｋ（ｔ）０,Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Ｇｅｎｅｒａｔｉｏｎ）ｔの更新キーであることを示す。

【０１０８】更新キーの配布処理ついて説明する。キーの更新は、例えば、図１３に示す有効化キーブロック（ＥＫＢ：Ｅｎａｂｌｉｎｇ Ｋｅｙ Ｂｌｏｃｋ）と呼ばれるブロックデータによって構成されるテーブルを、ネットワークを介して、あるいは記録媒体に格納してデバイス０，１，２に供給することによって実行される。なお、有効化キーブロック（ＥＫＢ）は、図１０に示されるようなツリー構造を構成する各リーフ（最下段のノード）に対応するデバイスに、新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック（ＥＫＢ）は、キー更新ブロック（ＫＲＢ：Ｋｅｙ Ｒｅｎｅｗａｌ Ｂｌｏｃｋ）と呼ばれることもある。

【０１０９】図１３に示す有効化キーブロック（ＥＫＢ）は、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図１３の例は、図１０に示すツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータである。図１０から明らかなように、デバイス０，デバイス１は、更新ノードキーとしてＫ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒが必要であり、デバイス２は、更新ノードキーとしてＫ（ｔ）００１，Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒが必要である。

【０１１０】図１３のＥＫＢに示されるように、ＥＫＢには複数の暗号化キーが含まれる。図１３の最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自身の持つリーフキーＫ００１０によってこの暗号化キーを復号し、更新ノードキーＫ（ｔ）００１を得ることができる。また、復号により得た更新ノードキーＫ（ｔ）００１を用いて、図１３の下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）が復号可能となり、更新ノードキーＫ（ｔ）００を得ることができる。

【０１１１】以下順次、図１３の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号することで、更新ノードキーＫ（ｔ）０が得られ、これを用いて、図１３の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号することで、更新ルートキーＫ（ｔ）Ｒが得られる。

【０１１２】一方、ノードキーＫ０００は更新する対象に含まれておらず、ノード０，１が、更新ノードキーとして必要なのは、Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒである。ノード０，１は、デバイスキーＫ０００，

Ｋ０００１を用いて、図１３の上から３段目の暗号化キーＥｎｃ（Ｋ０００，Ｋ（ｔ）００）を復号することで更新ノードキーＫ（ｔ）００を取得し、以下順次、図１３の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号することで、更新ノードキーＫ（ｔ）０を得、図１３の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号することで、更新ルートキーＫ（ｔ）Ｒを得る。このようにして、デバイス０，１，２は更新したキーＫ（ｔ）Ｒを得ることができる。

【０１１３】なお、図１３のインデックスは、図の右側の暗号化キーを復号するための復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【０１１４】図１０に示すツリー構造の上位段のノードキーＫ（ｔ）０，Ｋ（ｔ）Ｒの更新が不要であり、ノードキーＫ０００のみの更新処理が必要である場合には、図１４の有効化キーブロック（ＥＫＢ）を用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

【０１１５】図１４に示すＥＫＢは、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図１０に点線で示すグループ内のデバイス０，１，２，３がある記録媒体を用いており、新たな共通のコンテンツキーＫ（ｔ）ｃｏｎが必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて新たな共通の更新コンテンツキーＫ（ｔ）ｃｏｎを暗号化したしたデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｃｏｎ）が、図１４に示されるＥＫＢとともに配布される。この配布により、デバイス４など、その他のグループの機器が復号することができないデータとしての配布が可能となる。

【０１１６】すなわち、デバイス０，１，２はＥＫＢを処理して得たキーＫ（ｔ）００を用いて暗号文を復号すれば、ｔ時点でのコンテンツキーＫ（ｔ）ｃｏｎを得ることが可能になる。

【０１１７】図１５に、ｔ時点でのコンテンツキーＫ（ｔ）ｃｏｎを得る処理例として、Ｋ（ｔ）００を用いて新たな共通のコンテンツキーＫ（ｔ）ｃｏｎを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｃｏｎ）と、図１４に示すＥＫＢとを記録媒体を介して受領したデバイス０の処理を示す。すなわちこの例は、ＥＫＢによる暗号化メッセージデータをコンテンツキーＫ（ｔ）ｃｏｎとした例である。

【０１１８】図１５に示すように、デバイス０は、記録媒体に格納されている世代ｔ時点のＥＫＢと、自分があらかじめ格納しているノードキーＫ０００を用いて、上述したと同様のＥＫＢ処理により、ノードキーＫ（ｔ）００を生成する。さらに、デバイス０は、復号した更新ノードキーＫ（ｔ）００を用いて、更新コンテンツキーＫ（ｔ）ｃｏｎを復号して、後にそれを使用するために自分だけが持つリーフキーＫ００００で暗号化して格納する。

【０１１９】図１６に有効化キーブロック（ＥＫＢ）のフォーマット例を示す。バージョン６０１は、有効化キーブロック（ＥＫＢ）のバージョンを示す識別子である。なお、バージョンは、最新のＥＫＢを識別する機能と、コンテンツとの対応関係を示す機能を持つ。デプスは、有効化キーブロック（ＥＫＢ）の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ６０３は、有効化キーブロック（ＥＫＢ）中のデータ部６０６の位置を示すポインタであり、タグポインタ６０４はタグ部６０７の位置、署名ポインタ６０５は署名６０８の位置を示すポインタである。

【０１２０】データ部６０６は、例えば更新するノードキーを暗号化したデータを格納する。例えば図１５に示すような更新されたノードキーに関する各暗号化キー等を格納する。

【０１２１】タグ部６０７は、データ部６０６に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図１８を用いて説明する。

【０１２２】図１７では、データとして先に図１３で説明した有効化キーブロック（ＥＫＢ）を送付する例を示している。この時のデータは、図１７のＢで示す表に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この例の場合は、ルートキーの更新キーＫ（ｔ）Ｒが含まれているので、トップノードアドレスはKRとなる。このとき、例えば最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）は、図１７のＡで示す階層ツリーに示す位置Ｐ０に対応する。次の段のデータは、Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）であり、ツリー上では前のデータの左下の位置Ｐ００に対応する。ツリー構造の所定の位置から見て、その下に、データがある場合は、タグが０、ない場合はタグが１に設定される。タグは｛左（Ｌ）タグ，右（Ｒ）タグ｝として設定される。表Ｂの最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）に対応する位置Ｐ０の左下の位置Ｐ００にはデータがあるので、Ｌタグ＝０、右にはデータがないので、Ｒタグ＝１となる。以下、すべてのデータにタグが設定され、図１７のＣで示すデータ列、およびタグ列が構成される。

【０１２３】タグは、対応するデータＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）が、ツリー構造のどこに位置しているのかを示すために設定されるものである。データ部６０６に格納されるキーデータＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）・・・は、単純に暗号化されたキーの羅列データに過ぎないが、上述したタグによってデータとして格納された暗号化キーのツリー上の位置が判別可能となる。上述したタグを用いずに、先の図１５で説明した構成のよう

に、暗号化データに対応させたノード・インデックスを用いて、例えば、

０：Ｅｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）

００：Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）

０００：Ｅｎｃ（Ｋ（（ｔ）０００，Ｋ（ｔ）００）

・・・のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると、冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

【０１２４】図１６に戻って、ＥＫＢフォーマットについてさらに説明する。署名（Ｓｉｇｎａｔｕｒｅ）６０８は、有効化キーブロック（ＥＫＢ）を発行した例えば鍵管理センタ（ライセンスサーバ４）、コンテンツロバイダ（コンテンツサーバ３）、決済機関（課金サーバ５）等が実行する電子署名である。ＥＫＢを受領したデバイスは、署名検証によって正当な有効化キーブロック（ＥＫＢ）発行者が発行した有効化キーブロック（ＥＫＢ）であることを確認する。

【０１２５】以上のようにして、ライセンスサーバ４から供給された利用権に基づいて、コンテンツサーバ３から供給されたコンテンツを利用する処理をまとめると、図１８に示されるようになる。

【０１２６】すなわち、コンテンツサーバ３からクライアント１に対してコンテンツが提供されるとともに、ライセンスサーバ４からクライアント１にライセンスが与えられる。クライアント１をライセンスサーバ４に登録した際に供給されるサービスデータと、特定のコンテンツの利用を許可する情報である利用権との組み合わせをライセンスと呼ぶ。コンテンツは、コンテンツキーＫｃにより、暗号化されており（Ｅｎｃ（Ｋｃ，Ｃｏｎｔｅｎｔ））、コンテンツキーＫｃは、更新ルートキーＫＲ'(ＥＫＢから得られるキーであって、図５におけるキーK_{eeec}に対応する)で暗号化され（Ｅｎｃ（ＫＲ'，Ｋｃ））、ＥＫＢとともに、暗号化されたコンテンツに付加されてクライアント１に提供される。

【０１２７】図１８の例におけるＥＫＢには、例えば、図１９に示されるように、ＤＮＣで復号可能な更新ルートキーＫＲ'が含まれている（Ｅｎｃ（ＤＮＫ，ＫＲ'））。従って、クライアント１は、サービスデータに含まれるＤＮＫを利用して、ＥＫＢから更新ルートキーＫＲ'を得ることができる。さらに、更新ルートキーＫＲ'を用いて、Ｅｎｃ（ＫＲ'，Ｋｃ）からコンテンツキーＫｃを復号することができ、コンテンツキーＫｃを用いて、Ｅｎｃ（Ｋｃ，Ｃｏｎｔｅｎｔ）からコンテンツを復号することができる。

【０１２８】このように、クライアント１にＤＮＫを各デバイスに割り当てることにより、図１０と図１５を参照して説明した原理に従って、個々のクライアント１のリボーク（ｒｅｖｏｋｅ）が可能になる。

【０１２９】また、ライセンスリーフＩＤを付加して配布することにより、クライアント１において、サービスデータと利用権の対応付け照行われることになり、利用権の不正コピーを防止することが可能になる。

【０１３０】また、クライアント用の証明書と秘密鍵をサービスデータとして配信するようにすることで、エンドユーザも、これらを用いて不正コピーを防止可能なコンテンツを作成することが可能になる。

【０１３１】本発明においては、図１１を参照して説明したように、カテゴリノードにライセンスを管理するＴシステムと、各種のコンテンツを利用するデバイスのカテゴリが対応づけられるので、複数のＤＮＫを同一のデバイスに持たせることができる。その結果、異なるカテゴリのコンテンツを１つのデバイスで管理することが可能となる。

【０１３２】図２０は、この関係の一例を表している。すなわち、デバイスＤ１には、Ｔシステムに基づいて、ＤＮＫ１が割り当てられており、ＥＫＢを含むコンテンツ１を再生することができる。同様に、このデバイスＤ１には、例えば、ＤＮＫ２が割り当てられており、メモリースティックにＣＤからリッピングしたコンテンツ２を記録することができる。この場合、デバイスＤ１には、コンテンツ１とコンテンツ２という、異なるシステム（Ｔシステムとデバイス管理システム）により配信されたコンテンツを同時に扱うことが可能となる。新たなＤＮＫを割り当てるとき、既に割り当てられているＤＮＫを削除するなどして、デバイスに１個のＤＮＫだけを対応させるようにした場合、このようなことはできない。

【０１３３】このように、本発明においては、カテゴリ毎に独立したキー管理が可能になる。

【０１３４】また、ＤＮＫを、機器やメディアに予め埋め込むのではなく、ライセンスサーバ４により、登録処理を行う際に、各機器やメディアにダウンロードするようにすることで、ユーザによるキーの購入が可能なシステムを実現することができる。

【０１３５】コンテンツとその利用権を別々に配布するシステムにおいては、コンテンツは、それが作成された後、どのような使われ方をされようとも、その使われ方に関わりなく、全ての用途において、使用可能であるのが望ましい。例えば、異なるコンテンツ配信サービス、あるいは用途が異なる場合においても、同一のコンテンツが使えることが望ましい。本発明においては、このため、上述したように、各ユーザ（クライアント１）に、認証局としてのライセンスサーバ４から秘密鍵と、それに対応する公開鍵の証明書（ｃｅｒｔｉｆｉｃａｔｅｓ）が配布される。各ユーザは、その秘密鍵を用いて、署名（ｓｉｇｎａｔｕｒｅ）を作成し、コンテンツに付加して、コンテンツの真正さ（ｉｎｔｅｇｒｉｔｙ）を保証し、かつコンテンツの改竄防止を図ることができる。

【０１３６】次に、クライアント１から、クライアント

１に装着された、セキュアなメディアであり、コンテンツ記憶装置の一例であるメモリースティック（商標）へのコンテンツのチェックアウトの処理を説明する。

【０１３７】図２１は、メモリースティックの構成を示す図である。メモリースティック６５１は、フラッシュメモリ（不揮発性メモリ）６６１、メモリコントロールブロック６６２、およびＤＥＳ（Data Encryption Standard）の暗号化回路を含むセキュリティブロック６６３が１チップ上にＩＣ化されたものである。

【０１３８】フラッシュメモリ６６１は、メモリコントロールブロック６６２の制御の基に、符号化され、暗号化されたコンテンツを記憶する。

【０１３９】メモリコントロールブロック６６２は、シリアル／パラレル変換、またはパラレル／シリアル変換を実行すると共に、供給されたコマンドおよびデータとを分離して、分離されたコマンドを実行する。メモリコントロールブロック６６２は、供給されたコマンドに対応して、コンテンツをフラッシュメモリ６６１に記憶させるか、またはフラッシュメモリ６６１に記憶されているコンテンツを読み出す。

【０１４０】メモリースティック６５１のセキュリティブロック６６３は、複数の認証キーとメモリカード毎にユニークなストレージキーを記憶する。セキュリティブロック６６３は、乱数発生回路を有し、メモリコントロールブロック６６２の制御の基に、クライアント１と相互認証し、セッションキーを共有する。

【０１４１】セキュリティブロック６６３は、後述する使用条件およびＭＡＣ値を含むインデックスを記憶する。

【０１４２】セキュリティブロック６６３は、メモリコントロールブロック６６２の制御の基に、暗号化されているコンテンツを復号する。

【０１４３】図２２は、クライアント１によるコンテンツのチェックアウトの処理を説明するフローチャートである。

【０１４４】ステップＳ２０１において、クライアント１のCPU２１は、チェックアウトするコンテンツを選択して、選択したコンテンツに含まれる属性から署名を作成する。

【０１４５】例えば、クライアント１のCPU２１は、コンテンツに含まれる属性を、証明書に含まれるライセンスサーバの公開鍵で暗号化処理することにより、署名を作成する。

【０１４６】ステップＳ２０２において、クライアント１のCPU２１は、作成した属性の署名と、コンテンツに含まれる属性の署名とを比較し、作成した属性の署名と、コンテンツに含まれる属性の署名とが一致したと判定された場合、属性は改竄されていないので、ステップＳ２０３に進む。

【０１４７】ステップＳ２０２において、作成した属性の署名と、コンテンツに含まれる属性の署名とが一致しないと判定された場合、属性が改竄されているので、ステップＳ２０９に進み、クライアント１のCPU２１は、エラー表示などのエラー処理を実行し、チェックアウトの実行の処理を行わないで、処理は終了する。

【０１４８】ステップＳ２０３において、クライアント１のCPU２１は、対象となるコンテンツの属性が利用権に含まれるコンテンツ条件を満たし、チェックアウトが許可されている利用権を記憶部２８から検索する。対象のコンテンツを利用するための利用権が記憶部２８に見つからない場合には、ステップＳ２０９に進み、クライアント１のCPU２１はエラー表示などの、エラー処理を実行し、チェックアウトの実行の処理を行わないで、処理は終了する。

【０１４９】ステップＳ２０３において、コンテンツを利用するための利用権が見つかった場合には、Ｓ２０４に進み、クライアント１のCPU２１はコンテンツを利用するための利用権が記憶部２８に１つ記憶されているか、複数記憶されているかを判定する。

【０１５０】記憶部２８に対象のコンテンツを利用するための利用権が複数記憶されていると判定された場合、ステップＳ２０５に進み、クライアント１のCPU２１は、出力部２７のディスプレイに各利用権の使用条件等の情報を表示させ、どの利用権の使用条件をチェックアウトされたコンテンツの使用条件として用いるかをユーザに確認させ、ユーザからの入力部２６への入力を基に、いずれの利用権をチェックアウトに用いるかを決定する。

【０１５１】ステップＳ２０５における利用権の選択は、ユーザによる選択に限らず、所定の規則に基づき優先順位が決定されるようになっていても構わない。

【０１５２】記憶部２８に対象のコンテンツを利用するための利用権が１つ記憶されていると判定された場合、チェックアウトに用いられる利用権は決まっているので、ステップＳ２０５の利用権の選択は行われず、ステップＳ２０６に進む。

【０１５３】コンテンツを利用するための利用権の選択が行われた後、Ｓ２０６において、クライアント１のCPU２１は、利用権の使用条件から署名を作成する。

【０１５４】例えば、クライアント１のCPU２１は、利用権に含まれる使用条件を、証明書に含まれるライセンスサーバの公開鍵で暗号化処理することにより、署名を作成する。

【０１５５】ステップＳ２０７において、クライアント１のCPU２１は、作成した使用条件の署名と、利用権に含まれる使用条件の署名とを比較し、作成した使用条件の署名と、利用権に含まれる使用条件の署名とが一致したと判定された場合、使用条件は改竄されていないので、ステップＳ２０８に進む。ステップＳ２０８において、クライアント１のCPU２１は、チェックアウトの実

行の処理を行い、処理は終了する。

【０１５６】ステップＳ２０７において、作成した属性の署名と、コンテンツに含まれる属性の署名とが一致しないと判定された場合、属性が改竄されているので、ステップＳ２０９に進み、クライアント１のCPU２１は、エラー表示などのエラー処理を実行し、チェックアウトの実行の処理を行わないで、処理は終了する。

【０１５７】図２３は、ステップＳ２０８の処理に対応する、クライアント１のチェックアウトの実行の処理を説明するフローチャートである。

【０１５８】ステップＳ２２１において、クライアント１のCPU２１は、装着されているメモリースティックと相互認証の処理を実行する。例えば、クライアント１のCPU２１とメモリースティック６５１のセキュリティブロック６６３は、チャレンジアンドレスポンス方式の相互認証の処理を実行することができる。

【０１５９】ステップＳ２２１の処理において、相互認証されなかった場合、クライアント１またはメモリースティック６５１が、正当ではないので、ステップＳ２２２乃至Ｓ２２８の処理はスキップされ、コンテンツをメモリースティック６５１に書き込まないで、処理は終了する。

【０１６０】ステップＳ２２１の処理において、相互認証された場合、クライアント１およびメモリースティック６５１が、正当なので、クライアント１およびメモリースティック６５１は、共通の一時鍵（セッションキー）を共有し、ステップＳ２２２乃至Ｓ２２８の処理が実行される。

【０１６１】共通の一時鍵（セッションキー）が共有された以下の処理において、クライアント１がメモリースティック６５１に送信する情報は、暗号化復号部２４において、一時鍵で暗号化される。また、クライアント１がメモリースティック６５１から受信した情報は、一時鍵により暗号化されているので、暗号化復号部２４により、復号される。

【０１６２】ステップＳ２２２において、クライアント１のCPU２１は、コンテンツをメモリースティック６５１に書き込む。例えば、クライアント１のCPU２１は、メモリースティック６５１から、メモリースティック６５１のコンテンツキーを取得し、メモリースティック６５１のコンテンツキーに、コンテンツの鍵をかけ直して（コンテンツをメモリースティック６５１のコンテンツキーで暗号化して）、メモリースティック６５１のコンテンツキーに、鍵をかけ直したコンテンツをメモリースティック６５１に供給する。

【０１６３】なお、メモリースティック６５１に、コンテンツの鍵をかけ直させるようにしてもよい。

【０１６４】ステップＳ２２３において、クライアント１のCPU２１は、利用権の使用条件のフォーマットをメモリースティックに対応する方式に変換する。

【０１６５】ステップＳ２２４において、クライアント１のCPU２１は、暗号化復号部２４に、利用権の使用条件のメッセージ認証符号（MAC：Message authentication Code）（以下、ＭＡＣ値とも称する）を算出させる。

【０１６６】ＤＥＳ暗号処理構成を用いたＭＡＣ値生成例を図２４に示す。図２４の構成に示すように対象となるメッセージ（使用条件）を８バイト単位に分割し、（以下、分割されたメッセージをＭ１、Ｍ２、・・・、ＭＮとする）、まず、初期値（IV）とＭ１を、演算部２４－１Ａにより排他的論理和する（その結果をＩ１とする）。次に、Ｉ１をＤＥＳ暗号化部２４－１Ｂに入れ、鍵（以下、Ｋ１とする）を用いて暗号化する（出力をＥ１とする）。続けて、Ｅ１およびＭ２を演算部２４－２Ａにより排他的論理和し、その出力Ｉ２をＤＥＳ暗号化部２４－２Ｂへ入れ、鍵Ｋ１を用いて暗号化する（出力Ｅ２）。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。ＤＥＳ暗号化部２４－ＮＢから最後に出てきたＥＮがメッセージ認証符号（ＭＡＣ（Message Authentication Code））となる。

【０１６７】ステップＳ２２５において、クライアント１のCPU２１は、ステップＳ２２３の処理でフォーマットが変換された使用条件を、ステップＳ２２４の処理で算出されたＭＡＣ値と共にメモリースティック６５１のインデックスに書き込む。

【０１６８】図２５は、メモリースティック６５１に記憶されているインデックスおよびコンテンツを説明する図である。

【０１６９】メモリースティック６５１のインデックス７０１には、コンテンツに対応して、コンテンツの使用条件、ＭＡＣ値、およびポインタが格納される。インデックス７０１のポインタは、コンテンツのアドレスを格納している。

【０１７０】例えば、メモリースティック６５１に記憶されているコンテンツ７０２－１を示すポインタは、コンテンツ７０２－１の使用条件およびそのＭＡＣ値と共に、インデックス７０１に格納される。メモリースティック６５１に記憶されているコンテンツ７０２－２を示すポインタは、コンテンツ７０２－２の使用条件およびそのＭＡＣ値と共に、インデックス７０１に格納される。メモリースティック６５１に記憶されているコンテンツ７０２－３を示すポインタは、コンテンツ７０２－３の使用条件およびそのＭＡＣ値と共に、インデックス７０１に格納される。

【０１７１】ステップＳ２２６において、クライアント１のCPU２１は、メモリースティック６５１から、ステップＳ２２５の処理により、新たに使用条件およびＭＡＣ値が書き込まれたインデックス７０１を取得する。

【０１７２】ステップＳ２２７において、クライアント１のCPU２１は、新たに使用条件およびＭＡＣ値が書き

込まれたインデックス７０１を基に、メモリースティック６５１全体のインテグリティ・チェック値（ＩＣＶ）を算出する。

【０１７３】インデックス７０１のインテグリティ・チェック値は、例えばインデックス７０１に対するハッシュ関数を用いて計算され、ＩＣＶ＝ｈａｓｈ（Ｋｉｃｖ，Ｒ１，Ｒ２，・・・）によって計算される。ＫｉｃｖはＩＣＶ生成キーである。Ｌ１，Ｌ２は使用条件の情報であり、使用条件のＭＡＣ値が使用される。

【０１７４】ステップＳ２２８において、クライアント１のＣＰＵ２１は、メモリースティック６５１のインテグリティ・チェック値を、算出したインテグリティ・チェック値に書き換えて、処理は終了する。

【０１７５】例えば、クライアント１のＣＰＵ２１は、メモリースティック６５１から取得したインデックス７０１に含まれる、コンテンツ７０２－１乃至７０２－３に対応するＭＡＣ値を基に、インテグリティ・チェック値を算出する。

【０１７６】クライアント１のＣＰＵ２１は、図２５に示すように、メモリースティック６５１に、算出したインテグリティ・チェック値７０３を書き込む。

【０１７７】クライアント１は、インテグリティ・チェック値を一時鍵で暗号化して、メモリースティック６５１に送信する、いわゆる、ＳＡＣ（Ｓｅｃｕｒｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｈａｎｎｅｌ）を介して、インテグリティ・チェック値をメモリースティック６５１に送信する。

【０１７８】このようにすることで、メモリースティックには、インデックス７０１に対応した、インテグリティ・チェック値７０３が安全に格納されることになる。

【０１７９】例えばコンテンツ再生時にインデックス７０１を基に生成したＩＣＶと、使用条件に基づいて生成したＩＣＶ７０３とを比較して同一のＩＣＶが得られれば使用条件に改竄のないことが保証され、ＩＣＶが異なれば、改竄があったと判定される。

【０１８０】図２６のフローチャートを参照して、図２３に示すクライアント１のチェックアウトの実行の処理に対応する、メモリースティック６５１のチェックアウトの実行の処理を説明する。

【０１８１】ステップＳ２４１において、メモリースティック６５１のセキュリティブロック６６３は、クライアント１のステップＳ２２１の処理に対応して、クライアント１との相互認証の処理を実行する。

【０１８２】相互認証された場合、クライアント１およびメモリースティック６５１において、共通の一時鍵（セッションキー）が共有される。

【０１８３】共通の一時鍵（セッションキー）が共有された以下の処理において、メモリースティック６５１がクライアント１に送信する情報は、セキュリティブロック６６３において、一時鍵により暗号化される。また、メモリースティック６５１がクライアント１から受信した情報は、一時鍵により暗号化されているので、メモリースティック６５１のセキュリティブロック６６３は、暗号化されている情報を一時鍵で復号する。

【０１８４】ステップＳ２４２において、メモリースティック６５１のメモリコントロールブロック６６２は、ステップＳ２２２の処理を実行するクライアント１からコンテンツが送信されてくるので、このコンテンツを受信して、コンテンツをフラッシュメモリ６６１に記憶させる。

【０１８５】ステップＳ２４３において、メモリースティック６５１のメモリコントロールブロック６６２は、ステップＳ２２５の処理を実行するクライアント１からフォーマットが変換された使用条件が送信されてくるので、使用条件を受信し、受信した使用条件をセキュリティブロック６６３のインデックス７０１に書き込む。また、メモリースティック６５１は、使用条件に対応させて、ステップＳ２４２の処理で記憶したコンテンツを示すポインタをセキュリティブロック６６３のインデックス７０１に書き込む。

【０１８６】ステップＳ２４３の処理により、図２５に示すように、新たに記憶されたコンテンツに対応する使用条件、ＭＡＣ値、およびコンテンツを示すポインタが、セキュリティブロック６６３のインデックス７０１に格納されることになる。

【０１８７】ステップＳ２４４において、メモリースティック６５１のメモリコントロールブロック６６２は、クライアント１から要求があるので、インデックス７０１をセキュリティブロック６６３から読み出し、読み出したインデックス７０１をクライアントに送信する。ステップＳ２４４の処理で送信されたインデックス７０１を受信することにより、クライアント１は、ステップＳ２２６の処理において、インデックス７０１を取得できる。

【０１８８】ステップＳ２４５において、メモリースティック６５１は、ステップＳ２２８の処理を実行するクライアント１から、新たなＩＣＶが送信されてくるので、クライアント１から送信されたＩＣＶを受信して、受信したＩＣＶを基に、ＩＣＶを更新し、処理は終了する。

【０１８９】このように、integrity情報である公開鍵暗号による署名がコンテンツに付され、共通鍵暗号方式によるハッシュ値によるintegrity情報が、クライアントにより生成され、データ記憶媒体の使用条件に付される。コンテンツのintegrity情報と使用条件のintegrity情報とが合わせて１つの情報として、インデックス７０１として管理されることになる。

【０１９０】このように、クライアント１は、メモリースティックの処理能力が低くとも、メモリースティックにおいて、コンテンツの保護のレベルを低下させることなく、公開鍵暗号方式による署名が付いたコンテンツ

を、メモリースティックにチェックアウトすることができるようになる。

【０１９１】処理能力が低い端末機においても、同一のコンテンツを使用することができるようになる。これにより、特に、あらゆるデバイス同士が、コンテンツをやりとりできるようになる。

【０１９２】すなわち、コンテンツをメモリースティックに書き込むようにした場合には、メモリースティックにコンテンツを記憶させることができる。

【０１９３】電子署名が付されているコンテンツのコンテンツ記憶装置への書き込みを制御し、コンテンツを利用するために必要な利用権の使用条件をコンテンツ記憶装置に対応するフォーマットに変換し、フォーマットが変換された使用条件の改竄を検出するための使用条件改竄検出データを生成し、フォーマットが変換された使用条件および使用条件改竄検出データのコンテンツ記憶装置への書き込みを制御するようにした場合には、能力の低いメモリースティックにおいても、コンテンツを利用できるようになると共に、コンテンツが不正に利用されるのを確実に防止することができる。

【０１９４】コンテンツを記憶するメモリを設けるようにした場合には、コンテンツを記憶することができる。

【０１９５】また、情報処理装置から提供された、電子署名が付されているコンテンツの記憶を制御し、情報処理装置から供給された、使用条件、および使用条件の改竄を検出するための使用条件改竄検出データの記憶を制御するようにした場合には、能力が低い場合であっても、コンテンツを利用できるようになると共に、コンテンツが不正に利用されるのを確実に防止することができる。

【０１９６】コンテンツ記憶装置であるメモリースティックに記憶させるコンテンツを選択し、選択されたコンテンツに付された第１の電子署名の検証を行い、選択されたコンテンツの利用を許可する利用権を記憶し、記憶部２８から選択されたコンテンツに対応する利用権を検索し、検索された利用権に付された第２の電子署名の検証を行い、検索された利用権に含まれている情報に基づき改竄検出データを生成し、第１の検証結果、第２の検証結果によりコンテンツおよび利用権が改竄されていないと判定されたことを条件として、利用権と改竄検出データとコンテンツをコンテンツ記憶装置に出力するようにした場合には、能力の低いメモリースティックにおいても、コンテンツを利用できるようになると共に、コンテンツが不正に利用されるのを確実に防止することができる。

【０１９７】クライアントからメモリースティックにコンテンツをチェックアウトする例を説明したが、クライアントからメモリースティックにコンテンツをコピーするようにしても良く、コンテンツを移動するようにしても良い。

【０１９８】また、クライアントからメモリースティックにコンテンツをチェックアウトする例を説明したが、クライアントからコンテンツ記憶装置の他の例であるPDにコンテンツをチェックアウト、移動、またはコピーするようにしてもよい。

【０１９９】さらに、クライアントからPDに装着されているメモリースティックにコンテンツをチェックアウト、移動、またはコピーするようにしてもよい。この場合において、相互認証の処理は、クライアントおよびPDの間で実行され、PDおよびメモリースティックの間で実行される。

【０２００】本発明が適用されるクライアントは、いわゆるパーソナルコンピュータ以外に、PDA（Personal Digital Assistants）、携帯電話機、ゲーム端末機などとすることができる。

【０２０１】一連の処理をソフトウエアにより実行させる場合には、そのソフトウエアを構成するプログラムが、専用のハードウエアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【０２０２】この記録媒体は、図２に示されるように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク４１（フレキシブルディスクを含む）、光ディスク４２（CD-ROM(Compact Disk -Read Only Memory),DVD(Digital Versatile Disk)を含む）、光磁気ディスク４３（MD（Mini-Disk）（商標）を含む）、もしくは半導体メモリ４４などよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているROM２２や、記憶部２８に含まれるハードディスクなどで構成される。

【０２０３】なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０２０４】また、セキュリティに関連する処理を実行させるプログラムは、その処理を解析されるのを防ぐため、そのプログラム自体が暗号化されているのが望ましい。例えば、暗号処理などを行う処理については、そのプログラムをタンパーレジスタントモジュールとして構成することができる。

【０２０５】また、上記実施例では、コンテンツを利用するために必要な利用権を特定するためにコンテンツの属性と利用権のコンテンツ条件を用いたが、これに限らない。例えば、コンテンツに、該コンテンツを利用するために必要な利用権の利用権IDを含むようにしても良

く、この場合、コンテンツを指定すればそれを利用するために必要な利用権は一意に決まるため、両者のマッチングを決定する処理を行う必要はない。

【０２０６】

【発明の効果】以上のように、本発明によれば、コンテンツ記憶装置にコンテンツを記憶させることができる。

【０２０７】また、本発明によれば、能力の低いコンテンツ記憶装置においても、コンテンツを利用できるようにすると共に、コンテンツが不正に利用されるのを確実に防止することができる。

【図面の簡単な説明】

【図１】本発明を適用したコンテンツ提供システムの構成を示すブロック図である。

【図２】図１のクライアントの構成を示すブロック図である。

【図３】図１のクライアントのコンテンツのダウンロード処理を説明するフローチャートである。

【図４】図１のコンテンツサーバのコンテンツ提供処理を説明するフローチャートである。

【図５】図４のステップＳ２６におけるフォーマットの例を示す図である。

【図６】図１のクライアントのコンテンツ再生処理を説明するフローチャートである。

【図７】図６のステップＳ４３の利用権取得処理の詳細を説明するフローチャートである。

【図８】利用権の構成を示す図である。

【図９】図１のライセンスサーバの利用権提供の処理を説明するフローチャートである。

【図１０】キーの構成を説明する図である。

【図１１】カテゴリノードを説明する図である。

【図１２】ノードとデバイスの対応の具体例を示す図である。

【図１３】有効化キーブロックの構成を説明する図である。

【図１４】有効化キーブロックの構成を説明する図である。

【図１５】有効化キーブロックの利用を説明する図である。

【図１６】有効化キーブロックのフォーマットの例を示す図である。

【図１７】有効化キーブロックのタグの構成を説明する図である。

【図１８】DNKを用いたコンテンツの復号処理を説明する図である。

【図１９】有効化キーブロックの例を示す図である。

【図２０】複数のコンテンツの１つのデバイスに対する割り当てを説明する図である。

【図２１】メモリースティックの構成を示す図である。

【図２２】コンテンツのチェックアウトの処理を説明するフローチャートである。

【図２３】クライアントのチェックアウトの実行の処理を説明するフローチャートである。

【図２４】ＤＥＳ暗号処理構成を用いたＭＡＣ値生成例を示す図である。

【図２５】メモリースティックに記憶されているインデックスおよびコンテンツを説明する図である。

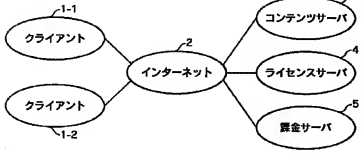
【図２６】メモリースティックのチェックアウトの実行の処理を説明するフローチャートである。

【符号の説明】

１－１，１－２　クライアント，　２　インターネット，　３　コンテンツサーバ，　４　ライセンスサーバ，　５　課金サーバ，　２０　タイマ，　２１CPU，　２４　暗号化復号部，　２５　コーデック部，　２６　入力部，　２７出力部，　２８　記憶部，　２９　通信部，　６５１　メモリースティック，６６１　フラッシュメモリ，　６６２　メモリコントロールブロック，　６６３　セキュリティブロック，　７０１　インデックス，　７０２－１乃至７０２－３　コンテンツ，　７０３　ＩＣＶ

【図１】

図1



【図１９】

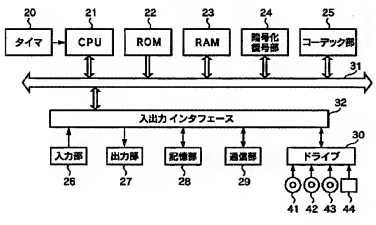
図19

EKB

Enc(DNK, KR)

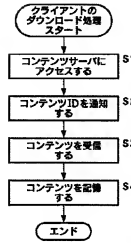
【図２】

図2



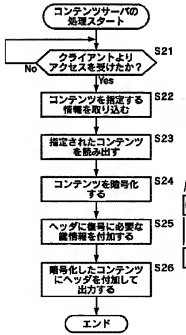
【図３】

図3



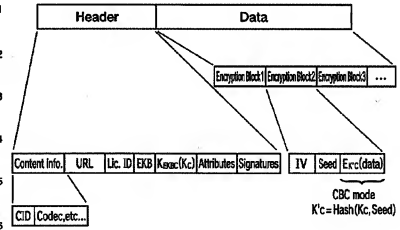
【図４】

図4



【図５】

図5



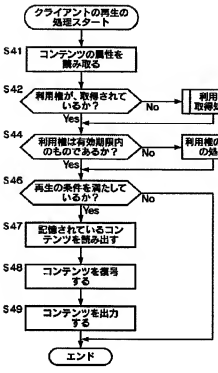
【図１３】

図13

バージョン(Version) :t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

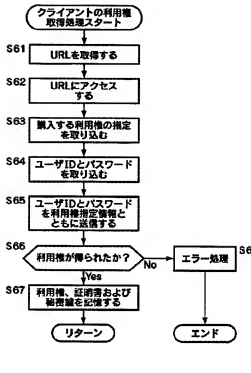
【図６】

図6



【図７】

図7



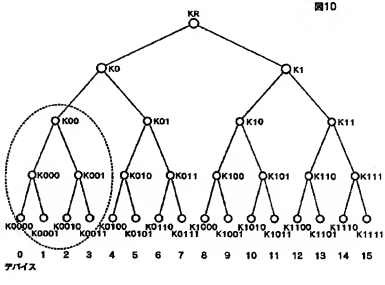
【図８】

図8

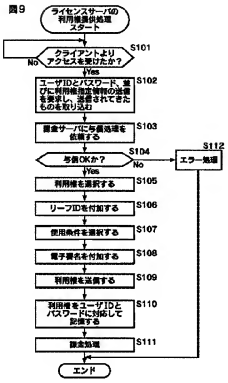
バージョン
プロファイル
利用権ID
作成日時
有効期限
使用条件
使用条件の電子署名
コンテンツ条件
定数
リーフID
電子署名
証明書

【図１０】

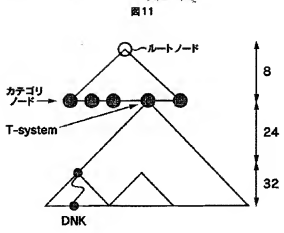
図10



【図９】



【図１１】

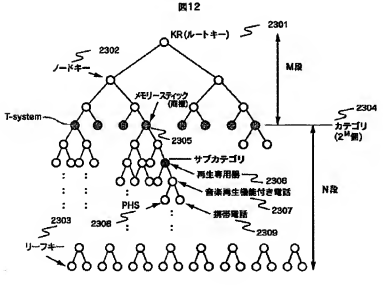


【図１４】

図14

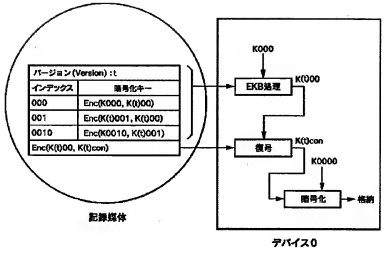
バージョン(Version) :t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

【図１２】



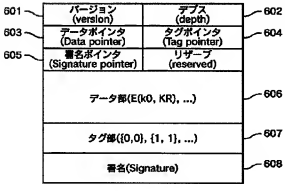
【図１５】

図15



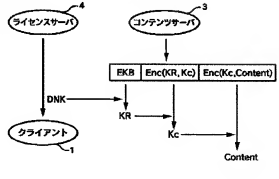
【図１６】

図16



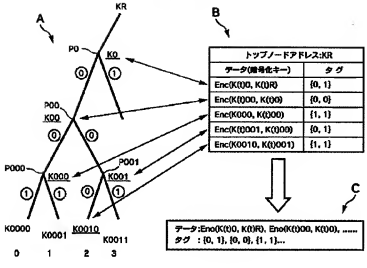
【図１８】

図18



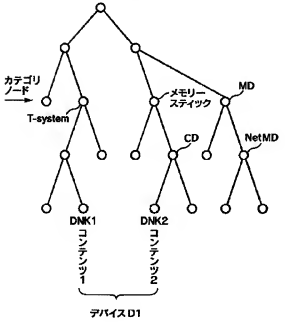
【図１７】

図17



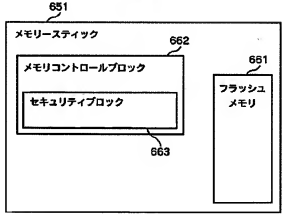
【図２０】

図20



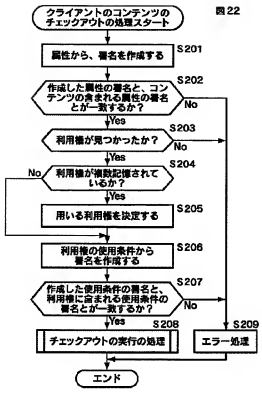
【図２１】

図21



【図２２】

図22

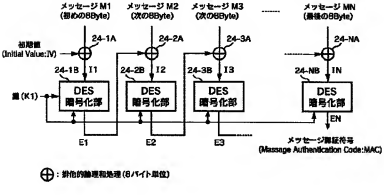


【図２３】

図23

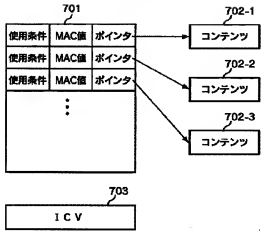
【図２４】

図24



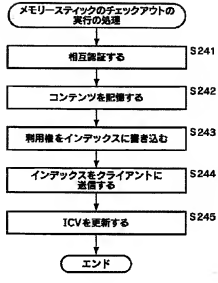
【図２５】

図25



【図２６】

図26



フロントページの続き

(72)発明者　二神　基誠
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Ｆターム(参考)　5B017 AA07 BA05 BA09 CA15 CA16
5J104 AA09 AA12 AA15 PA14